

Fordham Urban Law Journal

Volume 31 | Number 6

Article 5

2004

Hungry, Hungry HIPPA: When Privacy Regulations Go Too Far

Meredith Kapushion

Follow this and additional works at: <https://ir.lawnet.fordham.edu/ulj>



Part of the [Health Law and Policy Commons](#)

Recommended Citation

Meredith Kapushion, *Hungry, Hungry HIPPA: When Privacy Regulations Go Too Far*, 31 Fordham Urb. L.J. 1483 (2004).
Available at: <https://ir.lawnet.fordham.edu/ulj/vol31/iss6/5>

This Article is brought to you for free and open access by FLASH: The Fordham Law Archive of Scholarship and History. It has been accepted for inclusion in Fordham Urban Law Journal by an authorized editor of FLASH: The Fordham Law Archive of Scholarship and History. For more information, please contact tmelnick@law.fordham.edu.

Hungry, Hungry HIPPA: When Privacy Regulations Go Too Far

Cover Page Footnote

J.D. candidate, May 2005, Fordham University School of Law; B.A., Economics and Philosophy, Hillsdale College, 1999. The author acknowledges the contributions and support of Karol Boudreaux, Jay Cochran, and Susan Dudley at The Mercatus Center, George Mason University.

HUNGRY, HUNGRY HIPAA: WHEN PRIVACY REGULATIONS GO TOO FAR

Meredith Kapushion*

Privacy has many different definitions ranging from informational privacy to civil libertarian ideas of personal autonomy.¹ It is difficult to define as it arises from a complex set of rules and institutions which determine the limitations and availability of information.² As we find new ways to harness the massive amounts of available information, our lives may be subject to unwanted scrutiny and real losses stemming from privacy violations.³ While absolute privacy is unattainable, there are good reasons for pursuing policies which might prevent the erosion of its boundaries—no matter how gray or ill-defined those boundaries may be.⁴ In the area of personal health and medical information, the sensitive nature of the information at stake makes such losses all the more perilous and potentially injurious.⁵

Congress, concerned with the specter of privacy violations made possible by advances in technology and the use of electronic data storage, enacted medical privacy regulations with the Health Insur-

* J.D. candidate, May 2005, Fordham University School of Law; B.A., Economics and Philosophy, Hillsdale College, 1999. The author acknowledges the contributions and support of Karol Boudreaux, Jay Cochran, and Susan Dudley at The Mercatus Center, George Mason University.

1. See, e.g., Fred Cate, *Principles for Protecting Privacy*, 22 CATO J. 33, 34-36 (2002), available at <http://www.cato.org/pubs/journal/cj22n1/cj22n1-4.pdf>; Shaun Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 844-51 (2002).

2. See generally Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 123-30 (2004).

3. See generally Joy L. Pritts, *Developments and Trends in the Law: Altered States: Health Privacy Laws and the Impact of the Federal Health Privacy Rule*, 2 YALE J. HEALTH POL'Y L. & ETHICS 325, 329 (2002). For a laundry list of damaging privacy lapses, see Lois Collins, *Rx for Privacy*, DESERET NEWS, Sept. 2, 2001, at A1.

4. See generally Ernest Van Den Haag, *On Privacy*, in PRIVACY 149, 150-52 (J. Roland Pennock & John W. Chapman eds., 1971); Peter D. Jacobson, *Medical Records and HIPAA: Is It Too Late to Protect Privacy?*, 86 MINN. L. REV. 1497, 1499 (2002).

5. See, e.g., Fabio A. Sciarrino, *Ferguson v. City of Charleston: "The Doctor will See You Now, Be Sure to Bring Your Privacy Rights in With You!"*, 12 TEMP. POL. & CIV. RTS. L. REV. 197 (2002) (discussing case involving a South Carolina hospital that tested expectant mothers for drug use without disclosure and reported results to law enforcement); Spencer, *supra* note 1, at 887 nn.246-49 and accompanying text.

ance Portability and Accountability Act of 1996 ("HIPAA").⁶ HIPAA imposes considerable regulatory burdens on health care organizations in the hope that strict administration and control of information will prevent both real and perceived injuries from unauthorized and unwanted scrutiny of personal health data.⁷ These concerns are by no means unfounded, but it remains to be seen whether HIPAA's means of prevention are in fact the best cure.

Part I of this Comment traces a brief overview of the general development and regulatory requirements of HIPAA. Part II critiques HIPAA from a law and economics perspective, examining the economics of privacy, the problematic conditions in the market for health care services, whether HIPAA adequately addresses privacy concerns, and the costs and consequences of HIPAA. Part III suggests several alternatives for privacy advocates. In making policy choices, the costs should be carefully weighed against the benefits, and the outcomes should significantly solve the problems the policy was intended to address.⁸ The tradeoffs we accept in return for greater privacy protections should reflect our individual preferences to the greatest extent possible, and the solution put into place should have the flexibility to adjust to changing needs and the appropriate incentives to improve over time. Ultimately, HIPAA fails to meet these criteria, creates a number of new legal and economic problems, and adds regulatory and financial burdens to an already complex and costly health care system.

I. HIPAA's IMPLEMENTATION

While HIPAA's general policy goal was to protect the continuity of employee health coverage when changing jobs,⁹ the primary purpose of the privacy provisions was to address the public's concern over employer access to sensitive employee medical informa-

6. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) [hereinafter HIPAA].

7. See generally Lawrence Gostin & James Hodge, *The Nationalization of Health Information Privacy Protections*, 37 TORT & INS. L.J. 1113, 1113-15 (2002).

8. See Exec. Order No. 12,866, 58 Fed. Reg. 51,735 (Oct. 4, 1993), *amended by* Exec. Order No. 13,258, 67 Fed. Reg. 9,385 (Feb. 26, 2002).

9. HIPAA's preamble:

An Act to amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

HIPAA, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

tion.¹⁰ Other goals included providing additional safeguards against third party access to "protected health information" ("PHI"),¹¹ establishing procedures for information access,¹² and giving patients notice and access rights to their medical information.¹³

The HIPAA legislation gave Congress a self-imposed deadline of three years to enact legislation protecting the privacy of health information.¹⁴ Congress required the privacy regulations to address three specific areas:

- 1) The rights that an individual who is a subject of individually identifiable health information should have.
- 2) The procedures that should be established for the exercise of such rights.
- 3) The uses and disclosures of such information that should be authorized or required.¹⁵

In lieu of Congress meeting the deadline, the Secretary of Health and Human Services ("HHS") was authorized to enact such regulations.¹⁶ Congress failed to act before the HIPAA deadline in 1999. The HHS Secretary then undertook the task, issuing final regulations in April of 2001, which went into effect on April 14, 2003.¹⁷ Small group health plans (under \$5 million) were given an additional year to meet the requirements with April 16, 2004 as the

10. See generally Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. §§ 160, 164 (1999).

11. *Id.*

12. *Id.*

13. *Id.*

14. See HIPAA § 264(c)(1), Pub. L. 104-191, 110 Stat. 2033 (1996).

15. *Id.* § 264(b).

16. *Id.* § 264(a). Some legislative watchdogs claim that the timing of HIPAA combined with the three year deadline was driven by political gamesmanship. Both political parties hedged their bets that they would control the executive branch when the deadline was expected to pass, thereby allowing them to sidestep the legislative process in pursuit of their respective political agenda. See PRIVACILLA.ORG, HEALTH PRIVACY IN THE HANDS OF GOVERNMENT: THE HIPAA PRIVACY REGULATION—TROUBLED PROCESS, TROUBLING RESULTS 12 (2003), available at http://www.privacilla.org/releases/HIPAA_Report.pdf; see also Charlotte Twight, *Medicare's Progeny: The 1996 Health Care Legislation*, 2 INDEP. REV. 373, 373-74 (1998). But see Mary Grealy, *Health Privacy: The Beginning of the End or the End of the Beginning?*, CATO INST. HEALTH POL'Y STUDIES CONFERENCE 79, 80 (2001) (arguing that failure to meet the deadline was "due to issues like private right of action and the rights of minors"), available at <http://www.cato.org/events/transcripts/hipaa.pdf>; cf. Dick Armeey, *Just Gotta Learn From the Wrong Things You Done*, 22 CATO J. 7 (2002) ("HIPAA is a classic example of legislative panic."), available at <http://www.cato.org/pubs/journal/cj22n1/cj22n1-2.pdf>.

17. Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.534 (2004).

final deadline for compliance.¹⁸ The HHS rules regulate only covered entities—health care providers, insurers, health plans, and clearing houses which handle individually identifiable patient information and transmit that information electronically.¹⁹ The privacy provisions, however, cover all information regardless of format.²⁰ Electronic transmission is relevant only to determine whether an organization is a covered entity;²¹ covered entities are liable for all unauthorized disclosures of an individual's PHI, whether handled electronically or not.²²

The HIPAA provisions outline a number of penalties for non-compliance and wrongful disclosure of PHI. Disclosure penalties range from fines of \$100 to \$50,000 per violation.²³ Criminal penalties for violations with proven intent can include fines up to \$250,000 and ten years imprisonment.²⁴

Citing the need for reform and improving consumer confidence in the integrity of medical records, the regulations set forth uniform national standards for patient privacy protection. The evidence of privacy abuse, however, was largely anecdotal in nature, and many of the examples given were already in breach of law or contract and could not have been remedied, regardless of the policy in place.²⁵ Despite this, Congress took steps to deter potential future violations, and HIPAA marked the first time such a baseline national privacy standard had been promulgated.²⁶ The rules preempt state laws only to the extent that they are less prohibitive,²⁷ and do not replace them.²⁸ HIPAA intentionally creates a floor, but not a ceiling, on privacy protections in an attempt to provide consistent restrictions on the disclosure of PHI.

18. *Id.*

19. *Id.* § 160.103.

20. *Id.* § 164.501.

21. See *id.* § 160.103; see also Jeffrey Lovitsky, *Consents and Authorizations Under HIPAA*, 76 FLA. B.J. 10, 11 (2002).

22. See 45 C.F.R. §§ 164.501, 164.502(a).

23. See 42 U.S.C. § 1320d-6.

24. *Id.*

25. See PRIVACILLA.ORG, *supra* note 16, at 18.

26. See Rebecca Bishop, *The Final Patient Privacy Regulations Under the Health Insurance Portability and Accountability Act—Promoting Patient Privacy or Public Confusion?*, 37 GA. L. REV. 723, 735-36 (2003).

27. See *infra* notes 100-02 and accompanying text.

28. HIPAA, Pub. L. No. 104-191 § 2723, 110 Stat. 1936 (1996).

II. INTENT, EFFICIENCY, AND UNINTENDED CONSEQUENCES

A. The Economics of Privacy

It is difficult to treat privacy as a typical economic good. To fit the definition of an economic good, the quantity of privacy demanded must exceed the quantity supplied at a price of zero.²⁹ Simply put, if privacy were free, we would all want more. But what does this mean in the everyday world? There is no "market" for privacy per se,³⁰ and as a bundle of rules and institutions that limit the transferability of information, it is hard to think of privacy as a "good" the way that one thinks of apples, BMWs, or financial services as goods. Privacy is distinguished from the tangible goods which may complement it—window shades, caller I.D., trench coats, and fedoras—and from the substantive information it governs. The "bundle" is intangible, nontransferable, and possesses few, if any, of the characteristics we would traditionally ascribe to property.³¹

Despite fitting the model loosely, privacy is nonetheless an economic good.³² It is scarce, that is, we generally don't want to relinquish control over personal information unless we get something in return, and likewise, we would be willing to pay for more privacy up to the point where the marginal benefits equal the marginal costs.³³ As inapposite as it may initially seem, the metaphor of the market applies and it is instructive to think of privacy within the framework of supply and demand. The demand for privacy is driven by the competing consumption interests of market participants who would prefer other rules and institutions to govern the flow of information. Supply is similarly determined by the costs of ensuring more privacy.³⁴ In this context, market participants who

29. DAVID JOHNSON, PUBLIC CHOICE: AN INTRODUCTION TO THE NEW POLITICAL ECONOMY 26 (1991) ("[A]n economic good is one that is scarce relative to people's wants and, thus, commands a positive price on the market.")

30. A market for privacy *qua* privacy does not presently exist, although markets clearly do exist for goods and services which may give rise to greater privacy protection. Likewise, there are markets for personal information, but not for the rules and policies that govern those markets. In other words, there is, at present, no direct means for an individual to select or bargain for the conditions of their personal information market.

31. See, e.g., John Gould, *Privacy and the Economics of Information*, 9 J. LEGAL STUD. 827, 827-35 (1980).

32. See generally George Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623, 625 (1980).

33. See generally MURRAY ROTHBARD, *MAN, ECONOMY AND STATE* 241 (1962) (explaining marginal utility and principles of exchange).

34. Stigler, *supra* note 32, at 628.

value relaxed privacy protections will compete against those who favor more stringent policies.

As a brief aside, it is relevant to note that the current tone of the privacy debate leaves little wiggle room for those with competing demand interests. Fred Cate notes that

[i]t is frankly difficult to find the 'other' side of the privacy debate in large part because the benefits that result from open information flows (and may be placed at risk when privacy protections interfere with those flows) are so integral a part of our lives that they are seldom explicitly recognized or fully understood.³⁵

To avoid demonizing those who are "anti-privacy,"³⁶ it is useful to think of some of the positive effects of relaxed privacy standards from a broader social policy standpoint. For instance, fewer restrictions on information allow insurance markets to operate efficiently, reduce transaction costs among privacy providers, facilitate education and research, and lower overall costs for consumers.³⁷ These and other advantages benefit society in the aggregate and should not be easily discounted. The effect of any given privacy policy is to create a tradeoff between these benefits and those gained from limiting access to information.³⁸ Where the balance falls will depend on how we value these tradeoffs.³⁹ The important thing is that we are informed as we make these decisions and consider that an increase in the amount of privacy may be more harmful than beneficial after a certain point.⁴⁰

Privacy also presents another problem. While there may be a variety of options to choose from in buying any given privacy policy, the value of that policy is obscured until future valuations are revealed. Unlike most goods, the value of privacy is difficult to gage because damages from disclosure may be entirely unknown at the time the policy is agreed upon or "purchased," as is the likeli-

35. Cate, *supra* note 1, at 36.

36. Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, 2000 STAN. TECH. L. REV. 4, 5 (2000). "Just as no one is 'pro-abortion' or 'anti-life,' no one can be 'anti-privacy,' yet that's the only label left by the rhetoric." *Id.*

37. See Stigler, *supra* note 32, at 628-33.

38. See generally Lawrence Gostin & James Hodge, *Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule*, 86 MINN. L. REV. 1439, 1439-42 (2002).

39. *Id.*

40. See *infra* Part II.E.

hood of that disclosure occurring.⁴¹ Most consumers do not know what their future medical condition will be at the time they subscribe to a medical plan. They are essentially buying a "black box" based on risk preferences and speculation about future conditions based on limited present information. The acceptable risk of PHI disclosure is entirely unresolved until the substance of the PHI is known.⁴² Thus, the ultimate value of privacy is not revealed until long after a policy is in place.

Despite this drawback, privacy may still be treated as an economic good and priced as such. All time-preferenced goods involve some measure of risk evaluation and speculation in pricing.⁴³ Just as insurance policies reflect different risk preferences by offering an array of policies priced by actuarial estimates, so too can privacy policies reflect individual preferences by following a similar strategy.⁴⁴ One solution is to concentrate or bundle the preferences of individual consumers. This could take the form of group policy plans, provider set standards, or some hybrid between the two.

There is a problem, however, in that catering to individual preferences can become very costly, very quickly. While it is conceivable that an individual could contract with every covered entity they come into contact with, the costs could mushroom as providers scrambled to accommodate a variety of needs, and regulatory oversight is replaced by extensive contract enforcement. This is not a foregone conclusion, however. The incentive to develop a way to meet the need for customized solutions while keeping costs minimized is as strong as the demand driving it. Entrepreneurs in

41. See Richard Epstein, *HIPAA on Privacy: Its Intended and Unintended Consequences*, 22 CATO J., 13, 15 (2002) (noting that judgments are made behind a Rawlsian veil of ignorance) [hereinafter Epstein, *HIPAA on Privacy*], available at <http://www.cato.org/pubs/journal/cj22n1/cj22n1-3.pdf>.

42. For example, take a patient who is diagnosed with a condition that carries a costly social stigma. The value of keeping their medical information confidential escalates in proportion to the consequences of disclosure. The patient's demand for privacy at the time of "purchase" is substantially less than at the relevant time of policy enforcement.

43. See generally Mario Rizzo, *Time in Economics*, in THE ELGAR COMPANION TO AUSTRIAN ECONOMICS 111 (Peter Boettke ed., 1994).

44. The mechanics may be complex, but such a system would offer a variety of choices with greater flexibility on the part of providers and insurers, while ultimately leaving the decision in the hands of the consumer. Ideally, an array of competing policies would emerge to effectively meet the demands of a wide spectrum of consumers. Market pressures to supply the best product at the lowest cost would also tend to prevent unwanted information disclosures and minimize implementation and enforcement costs.

search of potential profits will search for ways to capitalize on the potential profits and will likely find innovative solutions.⁴⁵

Critics of this type of market-oriented approach point out that this kind of price discrimination is not possible within the current system because of "pervasive market failures."⁴⁶

Although they are correct in their assessment that the conditions for a traditional competitive market do not presently exist,⁴⁷ it is not a foregone conclusion that the market has failed or cannot provide an efficient outcome. Problems such as high transaction costs, information asymmetries, and bargaining power disparities are commonplace in the real world and many (if not all) economists are well aware that the theoretical constraints and *ceteris paribus* clauses that delimit economic models do not hold true in actual practice.⁴⁸ Despite this, markets tend to work, even when the conditions suggest the classical economics framework will have little predictive power.⁴⁹ Further, when particular markets are treated within an experimental framework, economists often discover that these discrepancies may not be problems at all.⁵⁰ This is not to say that the market always works flawlessly or that complications are irrelevant. Without looking at the actual functions of a particular market and at how the participants behave within the rules and institutions that exist, it is simply inaccurate to conclude that the underlying conditions inevitably lead to market failure or that there are not effective measures for changing the rules of the game in order to yield optimal outcomes.

With the advent of HIPAA, a uniform standard is imposed which cannot adjust to individual preferences without risking liability for

45. See generally Sanford Ikeda, *Market Processes* 23, 23-25 in *THE ELGAR COMPANION TO AUSTRIAN ECONOMICS* (Peter Boettke ed., 1994); Israel Kirzner, *Entrepreneurship*, 103, 103-110 in *THE ELGAR COMPANION TO AUSTRIAN ECONOMICS* (Peter Boettke ed., 1994).

46. See Spencer, *supra* note 1, at 891-907. But see JAY COCHRAN, *MERCATUS CTR., PUBLIC INTEREST COMMENT ON STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION* 13 (2001), available at <http://www.mercatus.org/pdf/materials/78.pdf> (noting that the HHS claim of market failure based on information asymmetry and externalities presupposes poorly defined property rights).

47. See, e.g., James Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 59-66 (2003).

48. See Mark Pauly, *Regulation of Bad Things That Almost Never Happen But Could: HIPAA and the Individual Insurance Market*, 22 CATO J. 59, 60-61 (2002) (discussing the problem of imperfect consumer information and insurance), available at <http://www.cato.org/pubs/journal/cj22n1/cj22n1-5.pdf>.

49. See, e.g., Vernon Smith, *Markets as Economizers of Information: Experimental Examination of the "Hayek Hypothesis,"* 20 ECON. INQUIRY 167, 167 (1982).

50. See *id.*

covered entities. Rather than enable more refined price discrimination by offering consumers a variety of choices priced along the demand curve, a "one-size-fits-all" federal policy ensures that there is no price discrimination whatsoever.⁵¹ Scarce resources are not allocated according to their most valued uses, and the benefits of a competitive market are lost to waste.⁵² HIPAA fails to match consumer preferences to competing policies, and the end result is guaranteed inefficiency and true market failure.

To illustrate part of the problem, consider a hypothetical hospital that caters only to patients with the lowest of privacy preferences. Even with all patients choosing to sign authorization and consent forms, the hospital would not escape the administrative and operative burdens that HIPAA imposes. The federal regulations mandate that the hospital jump through every compliance hoop, regardless of consumer preferences.⁵³ The patients end up bearing the financial costs of a system that offers them little or no substantial benefit.⁵⁴

In the real world, preferences are rarely so uniform.⁵⁵ Consumers have wildly divergent preferences based on their individual needs and tempered by the costs they are willing to bear. When patients have heterogeneous preferences, HIPAA is only able to cater to one segment of the market.⁵⁶ The costs are not borne in proportion to individual demand, and those with low privacy preferences end up subsidizing the privacy interests of those with high privacy preferences.⁵⁷ The net effect is a wealth transfer from the former group to the latter.⁵⁸

51. See PRIVACILLA.ORG, *supra* note 16, at 1.

52. For a discussion on the difficulty of obtaining market efficiency through central or government planning, see generally RICHARD MCKENZIE, *COMPETING VISIONS* (1985). McKenzie notes that the "economic problem" is not simply one of scarcity, but one of information coordination. *Id.* at 104-05, 108-12.

53. See generally Mary K. Martin, *Some Things Old, Some Things New: The HIPAA Health Information Privacy Regulations*, 59 BENCH & B. MINN. 32, 33-34 (2002); Elizabeth Morris et al., *HIPAA and Its Impact on Michigan's Health Professionals*, 81 MICH. B.J. 29 (2002).

54. See, e.g., Cate, *supra* note 1, at 38-43 (discussing the limits of notice and consent and comparing an opt-out to an opt-in rule).

55. See Richard Epstein, *A Taste for Privacy? Evolution and the Emergence of a Naturalistic Ethic*, 9 J. LEGAL STUD. 665, 679 (1980).

56. See generally Gary M. Anderson, *The Economic Theory of Regulation*, in THE ELGAR COMPANION TO AUSTRIAN ECONOMICS 294, 295-297 (Peter Boettke ed., 1994). In economic terms, this is a "deadweight loss," the uncaptured wealth that would otherwise be yielded in an efficient market.

57. See COCHRAN, *supra* note 46, at 5.

58. *Id.*

B. The Underlying Conditions of the Health Care Market

Stepping away from economic theory, it is useful to ask what led to the problems associated with medical privacy and health care providers in the first place. HIPAA was enacted to deal with the real conflict that exists between employee privacy and employer health care provision,⁵⁹ but how did this conflict arise? What led to the emergence of employer provision of health care? How did health care shift from a simple individual "fee for services" arrangement to a complex system of health plans, insurers, administrators, and federal regulation? The answer is not a simple one, but at least part of it lies in the Internal Revenue Code and the rise of third party payers.⁶⁰ Over time, policy changes and industry developments have shifted the role of purchasing and bargaining for medical services away from the consumer and towards employers, insurers, and group plan administrators.⁶¹ The tax code provides significant incentives for employers to manage and provide medical coverage as part of the package of benefits that employees receive.⁶² The tax burden for employer outlays is lower than if they paid the same amount to the employee directly,⁶³ and the resulting shift toward employer provision of medical benefits has become so commonplace that it is effectively mandatory in all but the lowest compensated occupations.⁶⁴

59. See generally PRIVACILLA.ORG, *supra* note 16, at 3.

60. *Id.* at 2.

61. See Victoria Craig Bruce, *Medical Savings Accounts: Progress and Problems Under HIPAA*, CATO POL'Y ANALYSIS, Aug. 8, 2001, at 1, available at <http://www.cato.org/pubs/pas/pa411.pdf>.

One of the major factors driving health care costs higher has been the increasing share of medical bills paid by third-party payers (private health insurers, employers, and government agencies) in the U.S. health care system. Most health care consumers do not pay directly for their own health care. Nearly 97 percent of hospital bills and more than 84 percent of physicians' fees are paid by private health insurance. On average, 80 cents of every dollar used to purchase health care is paid by someone other than the consumer who receives the care.

Id. at 3.

62. PRIVACILLA.ORG, *supra* note 16, at 3; see also JOHN GOODMAN & GERALD MUSGRAVE, NAT'L CTR. FOR POLICY ANALYSIS, CONTROLLING HEALTH CARE COSTS WITH MEDICAL SAVINGS ACCOUNTS (1992), available at <http://www.ncpa.org/pub/st/st168/>; S. Butler & C. Gavora, *How Tax Reforms Would Help Improve Patient Confidentiality*, HERITAGE FOUND. BACKGROUNDER, Jan. 19, 1999, at 3, available at <http://www.heritage.org/Research/Taxes/bgl1242.cfm>.

63. Butler & Gavora, *supra* note 62, at 3.

64. See generally Anne Maltz, *Health Insurance 101*, 690 PLI LIT. 523, 537-38 (2003).

While it may reduce individual transaction costs to seek jobs which bundle medical insurance with wages, this makes health services costlier overall.⁶⁵ At the margin, individuals have few incentives to either engage in risk-averse behavior or to keep claim costs low by monitoring the medical services they receive.⁶⁶ Depending on the particular type of health plan provided, employees may face strong incentives to consume more medical services, particularly if deductibles are low relative to individual demand and/or if individual account savings fail to roll over to successive periods. The more an individual is insulated from the costs of their choices, the more likely they are to spend.⁶⁷ Thus, plans with poor incentive structures result in greater costs overall. This free rider and collective action problem is remedied in part by the employers' interests in keeping costs low, but this indirect bargaining and monitoring is considerably less efficient than its direct alternative. The tradeoff between group plan savings and losses attributable to agency problems is complicated by tax incentives and the increasing complexity of insurance and benefits plans,⁶⁸ so it is unclear what the efficient market outcome would actually look like. It is almost certain, however, that if employers were given tax neutral treatment, third party payers would play a substantially smaller role.⁶⁹

As it stands, the current system places employers in the position of having to monitor the health services that are being provided to their employees. Without some sort of accountability check on the type and quality of care provided, employers have no means of keeping insurance costs down or monitoring what exactly they are paying for.⁷⁰ This creates a real dilemma for both employers and employees, as the tradeoff for accountability is the diminution of medical privacy. As one policy study notes:

65. See Butler & Gavora, *supra* note 62, at 4.

66. See GOODMAN & MUSGRAVE, *supra* note 62.

67. *Id.*

68. Consider, for example, the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 that, in subsidizing prescriptions, distances the payer from the beneficiary thereby creating additional distortion in the health care market. Medicare Prescription Drug, Improvement, and Modernization Act of 2003, Pub. L. 108-173, 117 Stat. 2066 (2003).

69. See generally M. Susan Marquis & Stephen Long, *To Offer or Not to Offer: The Role of Price in Employers' Health Insurance Decisions*, 36 HEALTH SERVICES RES. 935 (2001) (study finding that employer demand for health insurance is relatively inelastic with regards to changes in rate premiums and noting prior studies that have found varying results for studies based on the stated preferences of employers), available at <http://www.hospitalconnect.com/hsr/ArticleAbstracts/Marquis365.html>.

70. See Butler & Gavora, *supra* note 62, at 4.

Congress will not be able to address the privacy issue fully until it addresses the tax treatment of employer-provided health coverage. Providing tax credits directly to individuals so that they can purchase and own their own health insurance would vastly improve confidentiality of medical records and minimize regulatory intrusion into the patient-doctor relationship.⁷¹

This and other reform solutions are well worth considering before turning to more government regulation. If it were not for the tax code encouraging employers to play the awkward part of middleman in health care provision, many of the privacy concerns that led to the HIPAA legislation may never have arisen at all. The incidental benefit of changing the payment system to eliminate or reduce the roll of middlemen is to reduce the demand for information and thereby facilitate greater privacy protections.

C. HIPAA's Policy Failings

Unfortunately, HIPAA does little to address the accountability tradeoff, and largely fails to meet its own policy goal of establishing employer/employee privacy safeguards. Employers can effectively sidestep HIPAA's protections because of a number of broad consent exceptions⁷² and a lack of prohibitions on employers requiring PHI disclosure authorizations as a condition of employment.⁷³

71. *Id.*

72. See Charlotte Twight, *Prying Eyes: The End of Medical Privacy* (Jan. 21, 2003), at <http://www.foxnews.com/story/0,2933,76087,00.html> (last visited Oct. 20, 2004) [hereinafter Twight, *Prying Eyes*].

73. HHS also recognizes this problem:

Jeffrey Blair: [B]ut if we go back to the original thinking of why we needed privacy protections, if I recall correctly, the greatest concern that the public had was that their health care information might be inappropriately accessed by their employers. And that that might jeopardize either their ability to be hired, or their ability to retain their employment. Of course, HIPAA attempted to address this as well as it could within the framework that Congress gave us.

...

Mark Rothstein: [H]IPAA actually does really very little, if anything to address that problem that you referred to. That is, individuals being concerned that their employers have access to their health records. And the reason for that is it is lawful for an employer to require that an individual sign an authorization as a condition of employment, after the individual has received a conditional offer.

So, as a result, the disclosure of an individual's entire medical record to an employer is lawful under HIPAA. It's illegal in California and Minnesota, that have specific statutes that address this issue, but in the other 48 states, it's lawful. And so, therefore, HIPAA really doesn't help things. HIPAA will prevent the wrongful disclosure without an authorization, but as long as there was a valid authorization signed, there would not be a problem.

These and other exceptions may leave patients with inadequate privacy protections. Not only do the regulations open the door to the underprotection of privacy, the penalties often encourage draconian overenforcement of the regulations, in some cases, yielding *too much* privacy.⁷⁴

Given the morass of regulations and accreditation requirements that health care providers already have to contend with, it is not surprising that when faced with uncertainty or the prospect of liability, the tendency is to err on the side of caution and overenforcement.⁷⁵ When the stakes are high, uncertainty is an unappealing option, and covered entities are more likely to adopt reactionary policies that favor their interests over those of the patients they serve. A common example of this problem is often cited anecdotally: although the HIPAA rules require hospitals to allow patients to opt-out of the patient directory,⁷⁶ many hospitals treat it as an opt-in rule. Unless the patient explicitly authorizes the listing, hospitals will not reveal that information—even in the extreme situation where an unconscious and dying patient's friends and relatives are trying to locate her.⁷⁷ While some providers may be unknow-

Meeting transcript, HHS, National Committee on Vital Health Statistics (June 24, 2003), available at <http://www.ncvhs.hhs.gov/030624tr.htm>.

74. See, e.g., Kathleen Dracup & Christopher Bryan-Brown, Editorial, *The Law of Unintended Consequences*, 13 AM. J. CRITICAL CARE 97, 98 (2004). Dracup and Bryan-Brown state:

Horror stories are appearing in the literature, warning of unintended consequences. For example, a recent letter to the editor in the *New England Journal of Medicine* describes a situation in which a patient underwent cardiac transplantation. Postoperatively, routine blood cultures on the patient revealed a bacteremia. The infectious disease specialist at the recipient's hospital contacted the donor's hospital to ascertain the identity of the infection so that immediate antibiotic treatment could be initiated for the (now immunosuppressed) patient. The donor's hospital refused to release the information, citing HIPAA regulations and policies, because the (now deceased) donor had not given authorization for release of PHI.

Id.

75. *Id.*; see also Radly Balko, *The Barriers Don't Exist*, TECH CEN. STATION, June 4, 2004 (discussing the reluctance of insurers to price according to individual risk based on the false perception that federal regulations prohibit them from doing so), available at <http://www.techcentralstation.com/060404H.html>.

76. 45 C.F.R. §164.510(a)(2).

77. See Laurie Tarkan, *Sorry, That Information is Off Limits: A Privacy Law's Unintended Results*, N.Y. TIMES, June 3, 2002, at F5; see also Jack Rovner et al., *Managing the Privacy Challenge: Compliance with the Amended HIPAA Privacy Rule*, 15 HEALTH L. 18, 28-29 (2002); Yolanda Woodlee, *Hospital Bill is Family's Only Clue: Relatives Weren't Notified of Md. Man's Hit-and-Run Death*, WASH. POST, Jan. 20, 2004, at B5.

ingly misapplying the law, many knowingly overreach for fear of the litigation and penalties that threaten to ensue.⁷⁸

In a similar vein, consent forms tend to be overbroad to avoid potential liability.⁷⁹ While HIPAA takes steps to redress this by requiring plain language descriptions of the information and its means of disclosure,⁸⁰ it is largely ineffective given that few patients bother to read the authorization forms at all—much less in critical detail.⁸¹ While HIPAA shifts control towards patients, this is not clearly in their favor. They have the option to sign or not to sign, but they lose the diversity of options they have to choose from and may be left with a stark choice between relinquishing their privacy via a consent form or forgoing treatment altogether.

There are also numerous exceptions to the consent requirements that are not within the patient's control.

[T]oday patient consent is *not* required for disclosures of your personal medical information by covered entities in connection with medical treatment, payment or health care operations. Although patient authorization is required in certain other situations, a laundry list of over-broad exceptions retained from the original rules largely guts the authorization requirement.⁸²

The gains that might initially seem to advance the interests of ardent privacy advocates are quickly swallowed by this and other problematic HIPAA rules which inadequately protect patient privacy.⁸³

Privacy advocates should also be concerned with HIPAA's "transactions rule." The rule sets forth a standardized format for medical records,⁸⁴ which allows for centralized data collection on a scale not previously feasible. This move might bode well from a long-run cost-efficiency perspective, but it raises serious concerns

78. See Judith Graham, *Privacy Law a Bitter Pill*, CHI. TRIB., Apr. 13, 2004, at 1.

79. See Joseph Slobodzian, *Judge Upholds Changes to Medical-Privacy Law*, PHILADELPHIA INQUIRER, Apr. 3, 2004, at A12 ("Patients may refuse to sign the HIPAA form, but patient advocates argue that option is practically meaningless. Since the rule, advocates say, most doctors or medical providers refuse to assume civil and criminal liability for wrongly disclosed patient information and require patients to sign before they provide care.").

80. See Spencer, *supra* note 1, at 870-71.

81. See Cate, *supra* note 1, at 38.

82. Twight, *Prying Eyes*, *supra* note 72.

83. See *infra* text accompanying notes 97-102.

84. 45 C.F.R. §162.

for privacy.⁸⁵ Consider, for example, the failed proposal to create a National Data Center put forth by the Johnson administration.⁸⁶ What began as a proposal to consolidate agency efforts and cut back on costs turned into a behemoth database that would track individuals by consolidating nearly every piece of public information available on them in one location.⁸⁷ Following negative reactions from the public and Congress, the measure was abandoned on grounds of creating a security threat if the database were compromised and for putting civil liberties at risk.⁸⁸ These same concerns led to widespread opposition of Congress' plan to create a National Health Identifier ("NHI") as part of the original HIPAA legislation.⁸⁹ These requirements were copied almost verbatim from the rejected 1993 Clinton health security bill.⁹⁰ Although the NHI proposal was eventually withdrawn, similar threats to privacy remain as the security requirements of HIPAA dictate a standardized format for medical records, which includes Social Security numbers.⁹¹ In practice, if not in principle, this is essentially equivalent to the NHI proposal.⁹²

D. HIPAA's Costs

In addition to the structural problems outlined above, HIPAA also comes with a high price tag. There are direct and indirect costs of administration, as well as a number of hidden costs in the form of unintended consequences. Turning first to the direct costs, even the conservative HHS estimates are substantial. HHS estimated the start up costs of compliance at \$3.5 billion with continued annual costs of \$1.6 billion.⁹³ These cost estimates account for such sunk costs as initial policy development and implementation, renegotiation of contracts between business associates, technology improvements, and other administrative burdens.⁹⁴ Ongoing costs

85. See Charlotte Twight, *Health and Human Services "Privacy" Standards: The Coming Destruction of American Medical Privacy*, 6 INDEP. REV. 485, 486-88 (2002) [hereinafter Twight, *Health and Human Services*].

86. See Spencer, *supra* note 1, at 868.

87. *Id.*

88. *Id.*

89. See 64 F.R. 59,918, 59,921 (1999).

90. Twight, *Health and Human Services*, *supra* note 85, at 486.

91. *Id.* at 490.

92. *Id.* at 488.

93. See COCHRAN, *supra* note 46, at 3-4 (comparing HHS' estimates with independent cost estimates of \$4 billion and \$1.8 billion respectively, with a total long-run cost of roughly \$30 billion).

94. *Id.* at 2.

include personnel training, amendment and correction requirements, and patient authorizations.⁹⁵ Combined, these expenditures yield long-run baseline costs between \$25 and \$30 billion.⁹⁶

Along with direct expenditures, HIPAA also adds to the costs and inefficiencies of the health care market in the form of indirect costs. By adding a layer of regulatory red tape, HIPAA distorts the market process by introducing costs which disproportionately affect covered entities. While the rules may be the same for everyone, the costs of implementing them are not. Large insurance and health care companies will gain stronger positions in the market as they are more able to bear the costs of compliance. In contrast, small organizations will face greater proportional costs. HHS recognized this problem and gave an additional year for small health plans (not small providers) to comply, but this stopgap, applied only to a fraction of affected parties, does not address the underlying problem. The regulations also hinder new entrants to the market who now face higher start up costs as a result of the compliance requirements. These barriers to market entry make the market less competitive overall, and as the costs of entering and remaining in the market rise, so too do the costs of health care provision.⁹⁷

Lastly, HIPAA has a number of additional hidden costs in the form of unintended consequences. Some market players will invariably profit at the expense of others when new regulatory burdens take effect: here, there are a number of winners and losers. HIPAA is an economic boon to the tech industry⁹⁸ and to legal firms and others that specialize in HIPAA compliance.⁹⁹ Some in-

95. *Id.* at 3.

96. *Id.* at 4.

97. See Cass Sunstein, *Privacy and Medicine: A Comment*, 30 J. LEGAL STUD. 709, 713-24 (2001).

A serious danger is that a system designed to protect privacy, even in the way that is most sensible, might impose costs in excess of benefits, simply because it is so hard to manage. Time and effort are scarce commodities and far from trivial concerns. But the more important problem is that a burdensome system for the protection of privacy could undermine patient care itself, not least by making it more expensive.

98. See Peter Dizikes, *Tech Firms See New Medical Privacy Rules as Boon* (May 10, 2001), at <http://abcnews.go.com/sections/business/dailynews/medicalimaging010510.html> (last visited Oct. 20, 2004); Sandeep Junnarker, *Law Prescribes Overhaul of Imaging System*, (June 16, 2003), at http://news.com/2030-6681_3-1001641.html?tag=vs4_toc (last visited Oct. 20, 2004).

99. See, e.g., Jessica M. Lewis, *HIPAA: Demystifying the Implications for Financial Institutions*, 8 N.C. BANKING INST. 141, 156 n.133 (2004) (noting that Bank One gained a competitive edge by advertising itself as the first bank to become Claredi certified).

surance companies are already offering protections for liabilities derived explicitly from HIPAA violations.¹⁰⁰ While this may appear to create new jobs, it is only at the expense of scarce resources that would otherwise be put to use more efficiently elsewhere.¹⁰¹

The regulations also adversely affect charities and medical research. Charitable organizations that raise money for health causes depend on many former and current patients for charitable revenues.¹⁰² With the advent of HIPAA, they can no longer access or purchase targeted lists without patient consent.¹⁰³ This restraint puts charities devoted to medical illness and treatment that are dependent on individual donations at a significant disadvantage.¹⁰⁴ Likewise, HIPAA makes it more difficult for pharmaceutical companies, medical device manufacturers, epidemiologists,¹⁰⁵ and clinical researchers to conduct clinical trials.¹⁰⁶ Researchers no longer have easy access to the medical information that allows them to reach the relevant test subjects.¹⁰⁷ This hurdle will make the already lengthy and expensive delay between product invention and market availability even more encumbered.

Other industries may also face higher costs by virtue of falling with the "covered entities" category, even though they are not ostensibly part of the health care industry. Law firms,¹⁰⁸ banks,¹⁰⁹ and insurers (outside of health insurance), to name but a few, are

100. See Arnold Rosenbaum, *HIPAA Liability More than Meets the Eye*, HEALTH-IT WORLD (Nov. 13, 2003), at http://www.imakenews.com/health-itworld/e_article000200880.cfm (last visited Oct. 20, 2004).

101. See HENRY HAZLITT, *ECONOMICS IN ONE LESSON* 17 (3rd ed. 1978) ("The art of economics consists in looking not merely at the immediate but at the longer effects of any act or policy; it consists in tracing the consequences of that policy not merely for one group but for all groups.").

102. See Epstein, *HIPAA on Privacy*, *supra* note 41, at 15-16.

103. Tarkan, *supra* note 81; see also John Eggertsen et al., *HIPAA Privacy Regulations: A Summary*, SH078 ALI-ABA 29, 68 (2003).

104. Tarkan, *supra* note 81.

105. See American College of Epidemiology (ACE) *Testimony on Impact of HIPAA on Research, Before the Department of Health & Human Services' Nat'l Comm. on Vital Health Stats' Subcomm. on Privacy and Confidentiality* (Nov. 20, 2003) (remarks by Martha Linet, M.D., M.P.H., ACE President-Elect), available at <http://www.ncvhs.hhs.gov/031120p3.htm>.

106. See Lynne Glover, *Conducting Clinical Trials Made More Difficult by New Privacy Regs*, PITTSBURGH BUS. TIMES, June 6, 2003; see also Epstein, *HIPAA on Privacy*, *supra* note 41, at 18.

107. HHS has included certain exceptions for public health related activities. For a detailed discussion, see generally Diana M. Bontá et al., *The HIPAA Privacy Rule: Reviewing the Post-Compliance Impact on Public Health Practice and Research*, 31 J.L. MED. & ETHICS 70, 70-72 (2003).

108. See *infra* notes 121-23 and accompanying text.

109. See Lewis, *supra* note 99, at 141.

among those that will face additional costs. In turn, these costs will be transferred to consumers in the form of higher costs for legal and banking services, and higher insurance premiums. This “trickle down” effect is hard to trace and is unlikely to be fully accounted for in any HIPAA cost estimate.

E. HIPAA's Legal Problems

HIPAA also raises a number of legal problems. There are tricky issues with some of the more straightforward legal questions. For instance, when is there a violation? When does a plaintiff have standing, and, what are the possible remedies and defenses? In addition to these types of standard litigation questions, HIPAA raises issues that are unique—namely, problems related to the “minimum necessary” standard and state law preemption problems. The typical litigation problems are worth exploring, but are beyond the scope of this paper. It is worthwhile, however, to spend some time looking at the “minimum necessary” standard and preemption problems as they have already generated considerable debate in the literature and litigation in the courts.

The “minimum necessary” standard requires that a covered entity make reasonable efforts to limit PHI to the minimum necessary to accomplish the purpose of the use, disclosure, or request.¹¹⁰ This attempt to further limit the misuse of PHI creates one of the greatest compliance challenges for covered entities.¹¹¹ Even for routine and recurring disclosures or requests, covered entities must implement policies and procedures to meet the standard.¹¹² Aside from the implementation burden, the main problem with the standard is that it is remarkably vague. Commentators have argued that it is “contrary to sound medical practice” and “unworkable in daily treatment situations.”¹¹³ Although it has thus far survived constitutional challenges,¹¹⁴ this assurance offers little consolation to covered entities struggling to implement the rule.¹¹⁵ The inherent ambiguity of a “reasonableness” test combined with the near infinite number of facts and circumstances that factor into one’s subjective judgment create a dangerous pitfall for covered entities.

110. See 45 C.F.R. §164.502.

111. Jennifer Guthrie, *Time Is Running Out—The Burdens and Challenges of HIPAA Compliance: A Look at Preemption Analysis, the ‘Minimum Necessary’ Standard, and the Notice of Privacy Practices*, 12 ANNALS HEALTH L. 143, 158 (2003).

112. *Id.* at 160.

113. *Id.* at 159; see also Epstein, *HIPAA on Privacy*, *supra* note 41, at 25.

114. See *S.C. Med. Ass’n v. Thompson*, 327 F.3d 346, 355 (4th Cir. 2003).

115. See generally Guthrie, *supra* note 111, at 159-68.

In addition to the ambiguities of the "minimum necessary" requirement, HIPAA also creates state law preemption problems.¹¹⁶ The regulations call for federal preemption of state law except for a number of problematic exceptions. HIPAA does not preempt state law if the state law meets one of the following conditions:

- 1) Is necessary to prevent fraud and abuse;
- 2) Ensures appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation;
- 3) Allows for state reporting on health care delivery or costs;
- 4) Serves a compelling need related to public health, safety, or welfare, that warrants the intrusion into privacy when balanced against the need to be served;
- 5) Regulates the manufacture, registration, distribution, dispensing, or other control of any controlled substances, or that is deemed a controlled substance by state law;
- 6) Is more stringent than the HIPAA rule;
- 7) Provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation, or intervention; or
- 8) Requires a health plan to report, or to provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.¹¹⁷

Although these exceptions may seem benign on the surface, they cause considerable confusion as to when state law preempts the federal rule.¹¹⁸ The issues are not straightforward or easily dispensed with, and states are already seeing substantial litigation as courts address the issue.¹¹⁹ Until these issues are more firmly settled, we can only expect more of the same.

Regardless of the wisdom behind the preemption exceptions, much of the blame for generating this litigation falls squarely on HHS. Presumably to cut back on compliance costs, changes were

116. See generally J.S. Christie, Jr., *The HIPAA Privacy Rules From a Litigation Perspective*, 64 ALA. LAW. 126, 132 (2003).

117. See 45 C.F.R. § 160.203 (2001).

118. See generally Bishop, *supra* note 26, at 723.

119. See, e.g., *Law v. Zuckerman*, 307 F. Supp. 2d 705, 709 (D. Md. 2004) (finding preclusion where HIPAA is "more stringent" than Maryland's disclosure regulation); *Nat'l Abortion Fed'n v. Ashcroft*, No. 04 C 55, 2004 WL 292079, at *3 (N.D. Ill. Feb. 6, 2004) (stating that Illinois law supercedes HIPAA where state law has more restrictive disclosure requirements, even with a court ordered subpoena); *Lemieux v. Tandem Health Care*, 862 So.2d 745, 748 n.1 (Fla. Dist. Ct. App. 2003) (noting in dicta that Florida substantive law is more stringent than HIPAA on the issue of disclosure and thus Florida law supercedes the less protective federal regulations, even though HIPAA's procedural requirements are more stringent).

made to the final rule which eliminated a state's ability to seek out an advisory opinion on preemption.¹²⁰ While this reduces the burden on HHS, it fails to clarify the legal issues and merely shifts the burden onto courts to resolve the question at the state level.

Beyond the particular legal questions engendered by HIPAA, the regulations also invite new litigation. Although HIPAA does not create any new federal private rights of action for wrongful disclosures of PHI,¹²¹ the privacy standards are now being incorporated into state common law causes of action¹²² and may be used to extend actions to parties previously exempt for lack of privity.¹²³ For better or worse, this expansion of state law claims adds burdens to the court system and consumes legal resources.

There are also new legal costs outside of the claims themselves. Namely, lawyers face increased discovery costs and litigation obstacles in accessing medical records.¹²⁴ Attorneys also have greater internal compliance costs in the form of procedural safeguards for protecting client PHI, creating and monitoring arrangements with covered entities with respect to PHI, and in-house staff training.¹²⁵ When assessing HIPAA's legal costs, it would be a mistake to look simply at the damages awarded to successful plaintiffs or the costs of new claim litigation generally. The costs of HIPAA are much broader and ought to be accounted for. Resolving legal issues as a matter of first impression, working through more red tape during discovery, and adding encumbrances to law firms and attorneys must be added to the sum.

III. ALTERNATIVES

HIPAA's high costs, questionable benefits, and numerous economic, legal, and administrative consequences make a strong case for repeal. Not only does it seem reasonable to conclude that the benefits fail to exceed the costs, it may be that the policy may not

120. See Guthrie, *supra* note 111, at 155; Brian Zoeller, *Health and Human Services' Privacy Proposal: A Failed Attempt at Health Information Privacy Protection*, 40 BRANDEIS L.J. 1065, 1081 nn.90-91 and accompanying text.

121. See Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 618 (2002).

122. *Id.* at 652-58.

123. *Id.* at 662-65.

124. See Lori Baer & Christiana Callahan, *The Impact of HIPAA Privacy Regulations on Discovery of Plaintiffs' Medical Records*, 12 L.J.N'S PROD. LIAB. L. & STRATEGY 1 (2003).

125. See Alexander Gareeb, *Practical Implications of HIPAA*, 27 L.A. LAW 12 (2004).

produce *any* net benefits, *regardless* of cost.¹²⁶ As an alternative, we should consider less intrusive options that address the privacy concerns that led to HIPAA, while avoiding the many problems it has raised. A good solution meets the criteria of sound policy implementation,¹²⁷ while minimizing the regulatory costs and burdens.¹²⁸

Several possible solutions have already been noted: a broad re-examination of the structure of the health care payment system, a revision of the tax code,¹²⁹ and the development of a privacy insurance market.¹³⁰ The advantage of these types of reform is that they address certain underlying concerns of the health care market that regulatory reform generally neglects. The agency problems, poor incentive structures, collective action difficulties, and moral hazards that plague the health care system are at the root of rising costs and frustrations with medical coverage.¹³¹ Only by changing the rules of the game can we expect any real resolution to these problems. But, given that such reforms would require radical changes to the health care market and the current political climate, more incremental change seems likely.

Another possible route is to adopt clear guidelines for better privacy policies. Fred Cate sets forth one such framework. He suggests regulators "should focus on harm, not control; use narrow, precise definitions; employ appropriate consent requirements; apply regulations consistently; and evaluate the constitutionality of rules."¹³² Similarly, Cass Sunstein offers a narrower framework for evaluating health privacy:

A free society should begin with a strong presumption in favor of full patient control over personal information. The presumption is rebutted when disclosure to others is necessary (1) for good patient care, as in the case of consultations and medical teams; (2) to compile information that will produce scientific or

126. See Cate, *supra* note 1, at 37; Mike Koetting, *The Regulation of Managed Care Organizations and the Doctor-Patient Relationship*, 30 J. LEGAL STUD. 703, 703-04, 707 (2001).

127. See *supra* text accompanying note 8.

128. See also Epstein, *HIPAA on Privacy*, *supra* note 41, at 22-24 (discussing the public choice problems of HIPAA and the difficulties of reversing bureaucratic entrenchment).

129. See *supra* notes 57-68 and accompanying text.

130. See *supra* notes 43-49 and accompanying text.

131. See *supra* notes 59-69 and accompanying text.

132. Cate, *supra* note 1, at 53.

medical progress; (3) to protect third parties from serious risks of harm; and (4) to prevent harm to patients themselves.¹³³

Whether Cate or Sunstein has the right approach is debatable, but given the current regulatory environment and the promise of a better alternative, it may not be a bad idea to let their ideas play out. The current approach to privacy is muddled and simply not feasible. A more consistent and principled approach holds the promise of clarifying our legal rights and the value of those rights in any given tradeoff. At least with a clear sense of what is at stake, we can begin to make rational decisions about when, where, and how information ought to be handled.

As a final alternative, we may simply want to go back to the beginning. Prior to HIPAA, choices about privacy were exercised by those closest to the situation and circumstances, namely health care practitioners and intermediaries constrained by state privacy, contract, and tort laws.¹³⁴ They were also constrained by custom and common sense, norms we too often undervalue.¹³⁵ Not every solution to a problem need be a legal one, and the lack of widespread or systematic privacy abuse prior to HIPAA suggests there may not be a place for one.¹³⁶ Assuming, *arguendo*, that there is such a place, it may be best to bolster the protections that already exist for patient privacy at the state level, keeping in mind that there are significant tradeoffs to enhancing those protections.¹³⁷

Regardless of which path we take, there are good reasons for taking a more market-oriented approach. Among other things, it offers a variety of alternatives, eliminates or reduces the overall administrative burden, and removes the need for esoteric debates over what amount of privacy is the "right" amount for individual

133. Sunstein, *supra* note 97, at 710.

134. See Epstein, *HIPAA on Privacy*, *supra* note 41, at 20.

135. Sunstein suggests physician norms may be the best place to begin. See Sunstein, *supra* note 97, at 710.

136. See *supra* notes 25-26 and accompanying text.

137. See Epstein, *HIPAA on Privacy*, *supra* note 41, at 14.

The former [pre-HIPAA] world should not be treated as though it were the state of nature, in which no one knew about privacy or cared about the consequences that might flow from the inopportune release of information. Quite the opposite, the tradeoffs between the control of information and the need for its dissemination into different arenas did not first surface in 1995 or 1996. Rather, it has long been at the center of the discussion for research protocols used by physicians, hospitals, and research centers. The protection of medical records was always a big deal, one that was subject to regulation as well as contract.

consumers.¹³⁸ Although, the “invisible hand” of Adam Smith cannot point us to the solution, it does encourage innovation, choice, and most of all competition. We have no guaranteed means of knowing in advance who will win and who will lose, but it is important to set aside any pessimism, and remember that the openness of the market is precisely what makes it work.¹³⁹

As a corollary, it is also important to consider the benefits of competing legal regimes. By allowing states to experiment with different legal solutions that balance the privacy interests of consumers with the interests of the health care industry, we are more likely to see innovation and improvement.¹⁴⁰ State legislators can more readily change the laws when they become ineffective or excessive, and can more readily respond to the people affected. And, at least in principle, states can learn from each other and compare what does or does not make a system work and adjust accordingly. Under a uniform regime, we lose much of the incentive to create better laws at the state level. And although HHS officials may have the best of intentions, they face a much more difficult task in creating rules that best satisfy the conditions of each state's interests and existing legal framework. The agency is much less likely to finesse a solution that works for any single state, much less any particular health care market within that state.

CONCLUSION

In sum, HIPAA is not a good deal for patients, the health care industry, or any “covered entity” that has the misfortune to fall within its reach. The advantages of strengthening and simplifying the rules under a uniform standard are gained at the expense of experimentation and competition between states and among providers. The administrative burdens HIPAA imposes are, at best, a marginal benefit for a small segment of consumers. At its worst, HIPAA imposes costs directly and indirectly on nearly everyone and offers little in return. HIPAA's main agenda of resolving the employer/employee information disclosure problem remains

138. See, e.g., Jacobson, *supra* note 4, at 1506; cf. Sunstein, *supra* note 97, at 709-10.

139. See generally FRIEDRICH HAYEK, *INDIVIDUALISM AND ECONOMIC ORDER* 77-91 (1996).

140. See generally, Bruce Kobayashi & Larry Ribstein, *A Recipe for Cookies: State Regulation of Consumer Marketing Information*, at 1, 23-25, 36-38 (Prepared for the American Enterprise Institute, Federalism Project Roundtable on Internet Privacy, January 30, 2001) (discussing the advantages of state versus federal regulation in the context of consumer information privacy), available at <http://www.gmu.edu/departments/law/faculty/papers/docs/01-04.pdf>.

largely unresolved, and HIPAA does nothing to address the underlying agency problem. In place of a sound policy bolstering privacy protections, HHS has given us a stack of regulations that amount to a costly administrative headache with a number of wealth redistributive effects in tow. Alternatively, we should repeal HIPAA and consider less centralized, more competitive, and more effective options.